JAMES R. LANGEVIN
2D DISTRICT, RHODE ISLAND

COMMITTEE ON HOMELAND SECURITY
EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY
CHAIRMAN

BORDER, MARITIME, AND GLOBAL COUNTERTERRORISM

INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE
TERRORISM, HUMAN INTELLIGENCE, ANALYSIS AND COUNTERINTELLIGENCE

TECHNICAL AND TACTICAL INTELLIGENCE

Congress of the United States
House of Representatives
Washington, DC 20515–3902

WASHINGTON OFFICE:
109 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
TELEPHONE: (202) 225–2735
FAX: (202) 225–5976

DISTRICT OFFICE:
THE SUMMIT SOUTH
300 CENTERVILLE ROAD, SUITE 200
WARWICK, RI 02886
TELEPHONE: (401) 732–9400
FAX: (401) 737–2982

james.langevin@mail.house.gov
www.house.gov/langevin

The Honorable James R. Langevin

Opening Statement – "The Cyber Threat to Control Systems: Stronger Regulations are Necessary to Secure the Electric Grid"

Oct. 17, 2007

Today's hearing provides us with a prime opportunity to assess the future of cybersecurity and critical infrastructure protection in the United States. We will discuss two major issues today: the efforts to implement cybersecurity standards within the electric sector and a cyber vulnerability known as "Aurora" that was recently made public. I'll be blunt – if this Administration doesn't recognize and prioritize these problems soon, the future isn't going to be pretty.

The bulk power system of the United States and Canada has more than $1 trillion in asset value, more than 200,000 miles of transmission lines, and more than 800,000 megawatts of generating capability serving over 300 million people. The effective functioning of this infrastructure is highly dependent on control systems, which are computer-based systems used to monitor and control sensitive processes and physical functions. Once largely proprietary, closed-systems, control systems are becoming increasingly connected to open networks, such as corporate intranets and the Internet. As such, the cyber risk to these systems is increasing.

Intentional and unintentional control system failures on the bulk power system could have a significant and potentially devastating impact on the economy, public health, and national security of the U.S. For a society whose every function depends on reliable power, the disruption of electricity to chemical plants, banks, refineries, hospitals, water systems, and military installations presents a terrifying scenario. We will not accidentally stumble upon a solution to these problems. Instead, we must dedicate a lot of hard work and resources to secure our systems.

To this end, the Federal Energy Regulatory Corporation (FERC) has recommended protecting the bulk power system against disruptions from cyber attacks by approving a set of reliability standards developed by the North American Electric Reliability Corporation (NERC). The proposed standards require certain users, owners and operators of the grid to establish plans, protocols and controls to safeguard physical and electronic access to systems, to train personnel on security matters, to report security incidents, and to be prepared to recover information.

Two weeks ago Members of this Committee, including myself, Chairman Thompson, and Mr. McCaul, submitted comments to the FERC rulemaking. We believe that the standards proposed by NERC do not sufficiently ensure the production or delivery of

power in the event of intentional or unintentional cyber incidents involving critical infrastructures. The NERC standard focuses on the reliability of the bulk power system as a whole, ignoring the homeland security impact that loss of power in a region can have.

The standards won't cover a significant number of assets that are critical in providing power throughout the country. As several witnesses will testify today, the NERC standards won't require electric sector owners and operators to secure their generation units, distribution units, or telecommunications equipment. But we know from countless real world examples that these units are highly vulnerable to intentional and unintentional cyber events. Knocking any of these units off could affect the power supply to our nation's critical infrastructure.

Writing a standard that would preclude these elements just isn't good public policy. The technical experts agree with this assertion. According to research performed for NIST, the NERC standards are "inadequate for protecting critical national infrastructure." GAO concurs with those findings. I'm concerned about the narrow scope of the standards, particularly in light of recent events. CNN recently reported that DHS researchers at the Idaho National Laboratory successfully destroyed a generator through an experimental cyber attack. This experiment was code-named "Aurora."

Officials tell me that malicious actors – insiders, terrorists, or nation states – could use the same attack vector against larger generators and other critical rotating equipment that could cause widespread and long-term damage to the electric infrastructure. DHS, working through Idaho National Labs, and DOE have been developing mitigation measures for many of the critical infrastructure sectors. Naturally, we would expect owners and operators of critical infrastructure would mitigate these vulnerabilities as quickly as possible. Unfortunately, I have reason to believe that the mitigations developed by DHS and DOE have not been fully implemented across the electric sector.

Today, the Ranking Member and I sent a letter to FERC Chairman Joe Kelleher and asked him to commence an investigation to determine the extent to which electric sector owners and operators have implemented these mitigation efforts. Despite comments from industry that suggest otherwise, we in the Congress believe that this is a serious problem. This Subcommittee will continue its vigorous oversight over this critical aspect of our nation's homeland security.